

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-122931

(43)Date of publication of application : 28.04.2000

(51)Int.Cl.

G06F 12/14

G06F 9/06

H04L 9/10

(21)Application number : 10-293715

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 15.10.1998

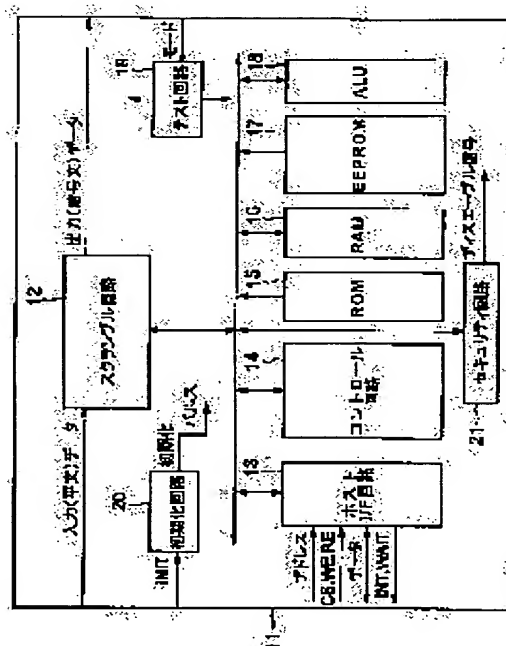
(72)Inventor : MOTAI MASAHIKO

## (54) DIGITAL INTEGRATED CIRCUIT

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To securely stop secret data from being accessed from outside and to easily perform reliable inspection at the time of a test by providing a control means which disables the external access to a specific storage area when specific data are written from outside.

**SOLUTION:** A ROM 15 stores fixed data such as open key data and programs. A RAM 16 provides an I/F area and a computing operation area for data communication with an external computer. Further, an EEPROM 17 functions to rewrite data different for every device and store data without a battery. Then a security circuit 21 as a control means performs control when certain specific data are inputted so that the area where secret data of each circuit part are written can not be accessed from outside. Before the specific data are inputted, respective circuit parts can freely be accessed from outside and a test can easily be conducted.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 ( J P )

(12) 公 開 特 許 公 報 ( A )

(11) 特許出願公開番号  
特開2000-122931  
( P2000-122931A )

(43) 公開日 平成12年 4 月28日 (2000. 4. 28)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 A 5 B 0 1 7
9/06	5 5 0	9/06	5 5 0 Z 5 B 0 7 6
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 A 5 J 1 0 4

審査請求 未請求 請求項の数10 O L (全 11 頁)

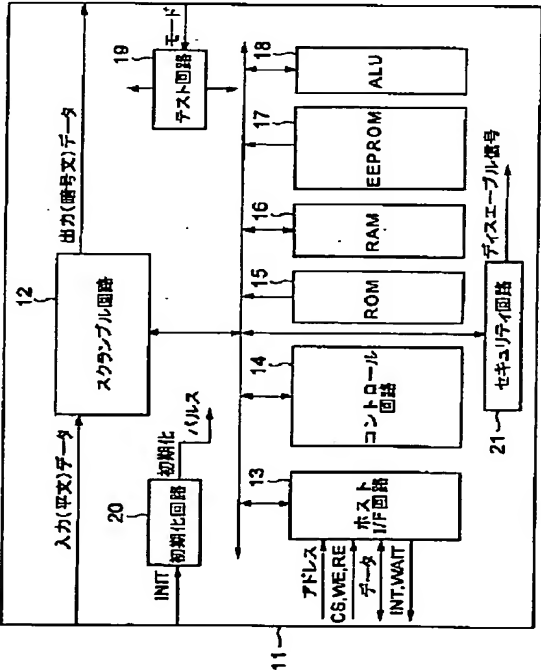
(21) 出願番号	特願平10-293715	(71) 出願人	000003078 株式会社東芝 神奈川県川崎市幸区堀川町72番地
(22) 出願日	平成10年10月15日 (1998. 10. 15)	(72) 発明者	馬渡 正彦 神奈川県川崎市幸区柳町70番地 株式会社 東芝柳町工場内
		(74) 代理人	100058479 弁理士 鈴江 武彦 (外 6 名)
		F ターム (参考)	5B017 AA01 BA01 BA07 BB03 CA12 5B076 AB10 CA08 FA02 FA14 5J104 AA01 AA16 EA08 NA27 NA39 NA43

(54) 【発明の名称】 デジタル集積回路

(57) 【要約】

【課題】この発明は、秘匿データに対しては外部からのアクセスを確実に阻止することができ、テスト時には信頼性の高い検査を容易に行ない得るようにしたデジタル集積回路を提供することを目的としている。

【解決手段】外部からのアクセスが可能で、内部に秘匿すべきデータが書き込まれる特定記憶領域を含む記憶手段15、16、17を備えたデジタル集積回路において、外部から特定データが書き込まれることにより、特定記憶領域への外部からのアクセスを不可とする制御手段21を備えている。



## 【特許請求の範囲】

【請求項 1】 外部からのアクセスが可能で、内部に秘匿すべきデータが書き込まれる特定記憶領域を含む記憶手段を備えたデジタル集積回路において、外部から特定データが書き込まれることにより、前記特定記憶領域への外部からのアクセスを不可とする制御手段を具備してなることを特徴とするデジタル集積回路。

【請求項 2】 前記制御手段は、前記特定データが書き込まれた状態で、その制御出力を外部から変更不能となることを特徴とする請求項 1 記載のデジタル集積回路。

【請求項 3】 前記制御手段は、前記特定データが書き込まれた状態で、その特定データの書き替えが不可となることを特徴とする請求項 1 記載のデジタル集積回路。

【請求項 4】 前記制御手段は、前記特定データが書き込まれた状態で、その特定データの書き替えが不可となるとともに、その制御出力を外部から変更不能となることを特徴とする請求項 1 記載のデジタル集積回路。

【請求項 5】 前記制御手段は、外部からデータが書き込まれるもので、データの書き込みが 1 回だけ可能なワンタイムメモリと、予め設定された固定データが記憶された記憶部と、この記憶部の固定データと前記ワンタイムメモリの内容とが一致した状態で、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力を発生する制御部とを具備してなることを特徴とする請求項 1 記載のデジタル集積回路。

【請求項 6】 前記制御手段は、外部からデータが書き込まれるメモリと、予め設定された固定データが記憶された記憶部と、この記憶部の固定データと前記メモリの内容とが一致した状態で、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力を発生するとともに、前記メモリに対する外部からのデータ書き込み及びデータ読み出しを不可とする制御部とを具備してなることを特徴とする請求項 1 記載のデジタル集積回路。

【請求項 7】 前記制御部は、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力に基づいて、前記メモリの書き込みイネーブル端を書き込み不能状態に設定するとともに、前記メモリから読み出しデータを外部に出力することを制限するゲート手段を遮断状態に設定することを特徴とする請求項 6 記載のデジタル集積回路。

【請求項 8】 前記制御手段は、外部から初期化が要求された状態で、前記記憶手段の特定記憶領域のアドレスを指定する指定手段と、この指定手段で指定されたアドレスに記憶された内容が書き込まれる第 1 の記憶部と、予め設定された固定データが記憶された第 2 の記憶部と、この第 2 の記憶部に記憶された固定データと前記第 1 の

記憶部の内容とが一致した状態で、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力を発生する制御部とを具備してなることを特徴とする請求項 1 記載のデジタル集積回路。

【請求項 9】 前記制御部は、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力が発生された状態で、前記記憶手段の記憶領域を、データの書き込み及び読み出しが共に可能な領域と、データの読み出しのみが可能な領域と、外部からのアクセスが不可な前記特定記憶領域とに分けることを特徴とする請求項 8 記載のデジタル集積回路。

【請求項 10】 前記記憶手段及び前記制御手段は、パッケージ内に封止されていることを特徴とする請求項 1 記載のデジタル集積回路。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、秘匿すべきデジタルデータを外部からアクセス不可能に保護するデジタル集積回路の改良に関する。

## 【0002】

【従来の技術】周知のように、例えばデジタルデータに暗号化処理を施すためのデジタル集積回路にあっては、暗号化処理の鍵となるデータや、その暗号化処理アルゴリズムを実行するためのプログラムデータ等のような秘匿すべきデータが、内部メモリに記憶されることになる。

【0003】この場合、デジタル集積回路には、その内部メモリ内に記憶された秘匿データが、外部から不正に読み出されたり書き替えられたりすることのないように、つまり、秘匿データを外部からアクセスすることが不可能になるように、保護対策が講じられている。

【0004】一方、この種のデジタル集積回路においては、工場で製造された後、その内部メモリを含む各種の内部回路が正常に動作するか否かを確かめるためのテストが行なわれる。このテストとしては、実際に各種の内部回路に所定のデータを入力して、期待した出力が得られる否かを確認する手法がとられている。

【0005】このため、上記したように、内部メモリに対して、そこに記憶されたデータを外部からアクセス不可能となるように保護対策が施されているという点と、製造時のテストを容易に行なえるようにする点とは、相反する技術となり、このことが、デジタル集積回路の設計製造を困難なものとしている。

【0006】通常、LSI (Large Scale Integrated circuit) 製造時の検査は、LSI テスターを用いて行なわれており、短時間で済ませることができ、しかも検査されていない回路部分を極力少なくすることが要求されている。特に、LSI 内部の RAM (Random Access Memory) の検査では、その全アドレスに渡って書き込みと読み出しとが正常に行なわれるか否かを調べる必要があ

10

20

30

40

50

る。

【0007】このためには、LSIの各回路部分毎にそれぞれテストモードを設定し、例えばRAMのテストモードを指定すると、RAMのアドレス端子とデータ端子とがLSIの接続ピンを介してテスターと接続され、また、暗号化処理のための特殊演算回路のテストモードを指定すると、その回路の入出力端子がLSIの接続ピンを介してテスターと接続されるように、LSIを設計している。

【0008】一方、外部からアクセス不可能となるように保護対策が施される回路部分については、LSI内部の素子を接続するワイヤーを電源端や接地端に接続して固定データを作り、公開された暗号の手續に沿ってのみテストを行なうことが可能になっている。また、検査途中のデータが外部に漏れないように、各回路部分の出力が外部に出ないように考慮されている。

【0009】このように、中間データをLSI外部に取り出すことができず、公開された暗号の手續に沿ってのみしかテストすることができないとなると、特定の回路を検査するのに複数の回路を経由しての検査となるため、テストのための入力データパターンが長くなるとともに、被検査部分の回路素子をできるだけ多く活性化させるということも困難になる。

【0010】特に、秘匿データが、1つ1つのLSI毎、あるいはそのLSIを搭載した1つ1つの機器毎に異なる場合には、例えば特開平7-45782号公報に示されるように、LSI毎あるいは機器毎に異なるデータを書き込み及び読み出しするためのデータチップと、暗号化処理するためのチップとを同一の基板上にモールドする等の処理が必要になってくる。

【0011】ここで、従来では、例えば特開平5-75597号公報等に示されるような、暗号処理LSICが提案されている。この暗号処理LSICは、秘匿データを記憶するメモリ部と、このメモリ部から読み出されるデータの外部への出力可否を制御する制御部と、メモリ部への秘匿データの書き込みアドレスを記憶する記憶部と、この記憶部に記憶された書き込みアドレスとメモリ部への読み出しアドレスとを比較する比較部とを備え、テストモードでかつ比較部の比較結果が一致した場合にのみ、制御部を出力可に制御するようにしたものである。

【0012】しかしながら、この暗号処理LSICでは、テストモードに設定されたとき、記憶部の全記憶内容がリセットされることが必要条件となる。このため、実際の使用状態において、何らかの原因でテストモードに投入されてしまうと、再度、メモリ部に秘匿データを書き込み、その書き込みアドレスを記憶部に記憶させるという作業が必要になるので、使用者にとって取り扱いが不便になるという問題が生じている。

【0013】

【発明が解決しようとする課題】以上のように、従来のデジタル集積回路では、秘匿データを外部からアクセス不可能となるように保護する点と、製造時のテストを容易に行なえるようにする点とが、それぞれ十分実用に供し得るレベルにまで達していないという問題を有している。

【0014】そこで、この発明は上記事情を考慮してなされたもので、秘匿データに対しては外部からのアクセスを確実に阻止することができ、テスト時には信頼性の高い検査を容易に行ない得るようにした極めて良好なデジタル集積回路を提供することを目的とする。

【0015】

【課題を解決するための手段】この発明に係るデジタル集積回路は、外部からのアクセスが可能で、内部に秘匿すべきデータが書き込まれる特定記憶領域を含む記憶手段を備えたものを対象としている。そして、外部から特定データが書き込まれることにより、特定記憶領域への外部からのアクセスを不可とする制御手段を備えるようにしたものである。

【0016】上記のような構成によれば、外部から特定データが書き込まれる前は、記憶手段に対して特定記憶領域も含めて外部からアクセス可能であるため、信頼性の高いテストを容易に行なうことができる。また、外部から特定データが書き込まれた後は、記憶手段の特定記憶領域が外部からアクセス不可となるので、秘匿データに対しては外部からのアクセスを確実に阻止することができる。

【0017】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して詳細に説明する。まず、図7は、この実施の形態で説明するデジタルLSIチップ10の外観を示している。このデジタルLSIチップ10は、以下に述べる各種の回路が形成された半導体基板11を樹脂製パッケージ内に封止してなる本体10aと、この本体10aから突出する複数のリード10bとから構成されている。

【0018】図1は、上記半導体基板11に形成された各種の回路を示している。まず、スクランブル回路12は、入力された明文データにスクランブル処理を施し、暗号文データに変換して出力している。

【0019】また、ホストI/F (Inter/Face) 回路13は、デジタルLSIチップ10の外部に設けられた図示しないコンピュータと通信を行なうためのインターフェースである。このホストI/F回路13は、コンピュータから送出されるアドレスデータ、チップセレクト信号CS、書き込みイネーブル信号WE及び読み出しイネーブル信号RE等を入力する機能と、データをコンピュータと双方向通信する機能と、割り込み信号INT及び待機信号WAIT等をコンピュータに出力する機能とを有している。

【0020】コントロール回路14は、デジタルLSIチップ10内部の制御や、暗号鍵解凍プログラムの演算制御を行なっている。ROM (Read Only Memory) 15は、公開鍵データやプログラム等の固定データを記憶している。RAM16は、外部コンピュータとのデータ通信を行なう際のI/Fエリアや、計算作業エリアを提供している。

【0021】さらに、EEP (Electrically Erasable and Programmable) ROM17は、機器毎に異なるデータを書き替え可能で、電池がなくてもデータを保存する機能を有している。ALU (Arithmetic Logical Unit) 18は、暗号化のための特殊演算を行なう特別の四則演算器である。

【0022】また、テスト回路19は、外部入力されるテストモード信号に基づいて、各回路部分を選択的にデジタルLSIチップ10の外部から検査し得る状態に切り替える。初期化回路20は、機器の電源投入時に供給される初期化要求信号INITに基づいて、各回路部分を初期化するための初期化パルスが発生する。

【0023】ここで、セキュリティ回路21は、詳細は後述するが、ある特定のデータが入力されると、各回路部分の秘匿データが書き込まれている領域を外部からアクセスすることができないように制御する。また、特定のデータが入力される前は、各回路部分が自由に外部からアクセスでき、テストを容易に行なえるようになっている。

【0024】図2は、上記ホストI/F回路13及びセキュリティ回路21の詳細な構成を示している。すなわち、ホストI/F回路13から出力される書き込みデータWDATAは、セキュリティ回路21のワнтаイムROM22の書き込みデータ入力端に供給されている。

【0025】このワнтаイムROM22は、1度だけのデータの書き込みを可能とする不揮発性メモリである。このワнтаイムROM22の読み出しデータ出力端は、そのビット毎に設けられた複数(図では簡単のため1個のみ示す)のEX (exclusive) オア回路23の一方の入力端に接続されている。

【0026】これらEXオア回路23の他方の入力端には、不揮発性のメモリ24に記憶された固定データが供給されている。これらEXオア回路23の各出力は、オア回路25によって論理和演算処理された後、フリップフロップ回路26にラッチされる。

【0027】すなわち、このEXオア回路23、オア回路24及びフリップフロップ回路26は、ワнтаイムROM22に書き込まれたデータと、メモリ24に記憶された固定データとの一致を判別している。そして、両データが一致している場合に、L (Low) レベルのディスエーブル信号が、セキュリティ回路21の出力として各回路部分に供給される。

【0028】また、このディスエーブル信号は、アンド

回路27に供給されて、ホストI/F回路13から出力される書き込みイネーブル信号WEと、ホストI/F回路13のアドレスデコーダ28から出力される第4のチップセレクト信号CS4と、論理積演算される。このアンド回路27の出力が、ワнтаイムROM22の書き込みイネーブル端に供給されている。

【0029】図2に示す構成において、まず、デジタルLSIチップ10の製造後の検査時には、ワнтаイムROM22には何もデータが書き込まれておらず、メモリ24の固定データとの一致がとられていないため、セキュリティ回路21からは、H (High) レベルのディスエーブル信号が出力されている。

【0030】この状態では、外部から各回路部分が自由にアクセスでき、容易にテストを行なうことができる。ただし、ワнтаイムROM22は、一旦データを書き込んでしまうと書き替えができないため、その書き込み読み出しテストは行なわれないようになされている。

【0031】テストが終了した後、その検査用のテストで直接に、または、外部コンピュータからホストI/F回路13を介して、ワнтаイムROM22に、メモリ24に記憶されている固定データと同じ値の特定データを書き込む。すると、ワнтаイムROM22に書き込まれたデータと、メモリ24の固定データとが一致するので、セキュリティ回路21からは、Lレベルのディスエーブル信号が出力される。

【0032】この状態では、デジタルLSIチップ10の各回路部分のうち、秘匿データが書き込まれている部分が外部からアクセスできないように設定される。そして、このようにワнтаイムROM22に、メモリ24に記憶されている固定データと同じ値の特定データが書き込まれると、ワнтаイムROM22の内容は書き替えることができないため、以後、ディスエーブル信号はLレベルに固定され、秘匿データが確実に保護されることになる。

【0033】図3は、上記したディスエーブル信号を発生するための他の例を示している。すなわち、セキュリティ回路21には、ワнтаイムROM22に代えてEEPROM29が設置されている。そして、ホストI/F回路13から出力される書き込みデータWDATAが、EEPROM29の書き込みデータ入力端に供給されている。

【0034】また、上記フリップフロップ回路26から出力されるディスエーブル信号と、ホストI/F回路13から出力される書き込みイネーブル信号WEと、ホストI/F回路13のアドレスデコーダ28から出力される第4のチップセレクト信号CS4とを論理積演算するアンド回路27の出力が、EEPROM29の書き込みイネーブル端に供給されている。

【0035】さらに、EEPROM29の読み出しデータ出力端は、上記EXオア回路23の一方の入力端に接

続されるとともに、3ステートバッファ30を介して、読み出しデータRDATAの伝送ラインに接続されている。

【0036】そして、フリップフロップ回路26から出力されるディスエーブル信号と、ホストI/F回路13から出力される読み出しイネーブル信号REと、ホストI/F回路13のアドレスデコード28から出力される第4のチップセレクト信号CS4とを論理積演算するアンド回路31の出力が、3ステートバッファ30のイネーブル端に供給されている。

【0037】図3に示す構成において、外部コンピュータによってセキュリティ回路21のEEPROM29に、メモリ24に記憶されている固定データと同じ値の特定データを書き込む。すると、EEPROM29に書き込まれたデータと、メモリ24の固定データとが一致するので、セキュリティ回路21からは、Lレベルのディスエーブル信号が出力される。

【0038】このようにして、ディスエーブル信号が一旦Lレベルになると、アンド回路27の出力、つまり、EEPROM29の書き込みイネーブル端がLレベルになるので、以後、EEPROM29に対するデータの書き換えは行なわれなくなる。

【0039】また、ディスエーブル信号が一旦Lレベルになると、アンド回路31の出力、つまり、3ステートバッファ30のイネーブル端がLレベルになるので、以後、EEPROM29から読み出された特定データが読み出しデータRDATAの伝送ラインに供給されないようになり、特定データが外部に読み出されることが防止されるようになる。

【0040】一方、デジタルLSIチップ10の製造直後のテスト時には、EEPROM29には何もデータが書き込まれていないので、EEPROM29のデータとメモリ24に記憶された固定データとは一致せず、ディスエーブル信号はHレベルとなっている。

【0041】このため、上記した特定データ以外のデータであれば、EEPROM29に対して、外部からのデータの書き込み及び読み出しが可能となり、EEPROM29のテストも容易に行なうことができる。

【0042】なお、図3に示した構成において、EEPROM29へのデータ書き込みに当たっては、同一データを繰り返し書き込む必要があるメモリもあり、この場合には、データの書き込みが完了するまでの期間中、フリップフロップ回路26の出力をHレベルに保持しておく必要があるが、その保持手段についての説明は省略する。

【0043】図4は、上記したディスエーブル信号を発生するためのさらに他の例を示している。すなわち、セキュリティ回路21には、ワンタイムROM22やEEPROM29に代えて、レジスタ32が設置されている。このレジスタ32は、そのデータ入力端が読み出し

データRDATAの伝送ラインに接続され、そのデータ出力端がEXオア回路23の一方の入力端に接続されている。また、このレジスタ32のクロック入力端には、初期化回路20から出力されるストロブ信号が供給されている。

【0044】また、セキュリティ回路21には、ロジック回路33が設置されている。このロジック回路33は、ホストI/F回路13から出力される書き込みイネーブル信号WE、読み出しイネーブル信号RE、第1乃至第3のチップセレクト信号CS1~CS3と、フリップフロップ回路26から出力されるディスエーブル信号と、初期化回路20から出力される初期化パルスとに基づいて、前記EEPROM17に対する、チップセレクト信号CS、書き込みイネーブル信号WE及び読み出しイネーブル信号REを生成している。

【0045】なお、このEEPROM17は、その書き込みデータ入力端が書き込みデータWDATAの伝送ラインに接続され、その読み出しデータ出力端が読み出しデータRDATAの伝送ラインに接続されている。

【0046】さらに、セキュリティ回路21は、EEPROM17の特定のアドレスA1を指定するためのアドレスデータが書き込まれたメモリ34を有しており、このメモリ34に書き込まれたアドレスデータと、ホストI/F回路13から出力される下位アドレスデータとが、初期化パルスで制御されるスイッチ35によって選択的にEEPROM17に導かれるようになっている。

【0047】ここで、上記ロジック回路33では、CS出力=CS1+CS2+CS3+初期化パルスのバー、WE出力=(CS1+CS2\*ディスエーブル信号+CS3\*ディスエーブル信号)\*入力WE、RE出力=(CS1+CS2+CS3\*ディスエーブル信号)\*入力RE+(初期化パルスのバー)なる演算を行なうことにより、チップセレクト信号CS、書き込みイネーブル信号WE及び読み出しイネーブル信号REをそれぞれ生成している。

【0048】図4に示す構成において、製造直後のテスト時に初期化回路20に初期化要求信号INITを供給すると、初期化回路20は、Lレベルの初期化パルスを発生する。すると、スイッチ35は、メモリ34側に切り替わり、メモリ34に記憶されているアドレスデータがEEPROM17に供給される。

【0049】また、この時点では、ホストI/F回路13から出力される書き込みイネーブル信号WEと読み出しイネーブル信号は共にLレベルで、チップセレクト信号CS1~CS3は不定であり、フリップフロップ回路26から出力されるディスエーブル信号はHレベルとなっているが、初期化パルスがLレベルであるために、ロジック回路33からは、Hレベルのチップセレクト信号、Lレベルの書き込みイネーブル信号、Hレベルの読み出しイネーブル信号が出力される。

【0050】このため、EEPROM17は、アドレスA1に記憶されているデータ（現時点では何も書かれていない）の読み出し状態となり、読み出されたデータが読み出しデータRDATAの伝送ラインに出力されることになる。

【0051】その後、初期化回路20に対する初期化要求信号INITの供給が停止されると、初期化回路20からは、1クロック期間分Hレベルとなるストロブ信号が発生されるので、読み出しデータRDATAの伝送ラインに出力されていたデータが、レジスタ32にラッチされる。そして、これよりさらに1クロック期間経過後、初期化パルスがHレベルになるので、スイッチ35が下位アドレスデータの伝送ライン側に切り替えられる。

【0052】この場合、レジスタ32にラッチされたデータは何も書かれていなかった値であるから、メモリ24の固定データとは一致せず、フリップフロップ回路26からはHレベルのディスエーブル信号が出力される。すると、ロジック回路33では、上式の演算が、CS出力=CS1+CS2+CS3、WE出力=(CS1+CS2+CS3)\*入力WE、RE出力=(CS1+CS2+CS3)\*入力REとなる。つまり、EEPROM17の全アドレス領域が外部からアクセス可能になり、テストが容易に行なわれる状態となる。

【0053】この状態で、EEPROM17のアドレスA1に、メモリ24に記憶されている固定データと同じ値の特定データを書き込み、再度、初期化回路20に対して初期化要求信号を供給して停止させる。すると、今度は、EEPROM17のアドレスA1に記憶されている特定データがレジスタ32にラッチされることになり、その結果、フリップフロップ回路26からはLレベルのディスエーブル信号が出力されることになる。

【0054】このとき、ロジック回路33では、上式の演算が、CS出力=CS1+CS2+CS3、WE出力=CS1\*入力WE、RE出力=(CS1+CS2)\*入力REとなる。つまり、EEPROM17に対し、チップセレクト信号CS1で指定される領域について書き込み及び読み出しを可能とし、チップセレクト信号CS2で指定される領域について書き込み不可で読み出しを可能とし、チップセレクト信号CS3で指定される領域について書き込み及び読み出しを不可とするように制御している。

【0055】図5(a)は、EEPROM17のアクセス領域を示している。図中上部がアドレス値の小さい領域であるとする。外部から指定されたアドレスに基づいて、ホストI/F回路13で生成されたチップセレクト信号CS1で指定される領域では、外部からの読み出しと書き込みとが共に可能となっている。

【0056】また、外部から指定されたアドレスに基づいて、ホストI/F回路13で生成されたチップセレクト

ト信号CS2で指定される領域では、外部からの読み出しのみが可能となっている。さらに、外部から指定されたアドレスに基づいて、ホストI/F回路13で生成されたチップセレクト信号CS3で指定される領域では、外部からの読み出しと書き込みとが共に不可となっている。

【0057】そして、前記メモリ34に書き込まれているアドレスA1は、チップセレクト信号CS3で指定される領域のアドレスとなっている。このため、チップセレクト信号CS3で指定される領域に秘匿データを書き込み、アドレスA1に固定データと同じ特定データを書き込んで、初期化することにより、秘匿データを外部からアクセス不可能にすることができる。

【0058】このようなEEPROM17のアクセス不能領域には、秘密を要する鍵データや暗号の非公開パラメータ、あるいは非公開の暗号処理アルゴリズムの実行プログラム等を書き込むことが有効である。また、EEPROM17の読み出し可能領域には、公開鍵データ等を書き込むことが有効である。

【0059】暗号の非公開パラメータには、機器毎に値が異なるデータと、機器毎には同一値となるデータとがあり、後者のデータは、図1に示したROM15に書き込むことも可能であるが、EEPROM17のアクセス不能領域に書き込む方が望ましい。

【0060】なぜならば、ROM15に書き込んだ場合、EEPROM17のアドレスA1に書き込んだ特定データが、何らかの原因で固定データと異なる値に変化して記憶されてしまうと、ROM15が外部からアクセス可能となって秘匿データが読み出されることになる。

【0061】これに対し、EEPROM17のアクセス不能領域に書き込むと、製造検査が可能となるだけでなく、EEPROM17のアクセス不能領域に書き込まれたデータが何らかの原因で変化する場合には、同一領域に書き込まれた他の非公開データも同じように変化していると考えられるので、元の正規の非公開データが読み出されることは防止することができる。

【0062】図5(b)は、デジタルLSIチップ10内のRAM16のアクセス領域を示している。このRAM16に対しても、EEPROM17の場合と同様に、チップセレクト信号CSiで指定される外部からの読み出し書き込み可能領域と、チップセレクト信号CSi+1で指定される外部からの読み出しのみ可能領域と、チップセレクト信号CSi+2で指定される外部からのアクセス不可領域とを設定することができる。

【0063】そして、例えば、このRAM16の読み出し書き込み可能領域は、外部とのデータ通信領域として使用され、読み出しのみ可能領域は、内部状態を示すフラグ等の記憶領域として使用され、アクセス不能領域は、暗号処理時における中間データ等の非公開データを処理するために使用される。

10

20

30

40

50



【0064】図6は、スクランブル処理における、そのテストと秘匿データの保護について説明している。すなわち、スクランブル回路12は、入力データにスクランブル処理を施すシャッフル回路12aと、ホストI/F回路13やコントロール回路14からのアドレスをデコードするアドレスデコーダ12bと、スクランブルキーを書き込むレジスタ12cと、スクランブルのモードを決めるコントロールレジスタ12dと、スクランブル回路12の状態や入力データの状態を示す状態レジスタ12eとを含んでいる。

【0065】また、コントロール回路14は、ゼネラルレジスタ14aと、命令レジスタ14bと、アドレス発生器14cとを含んでいる。さらに、暗号鍵解凍のための特殊演算器であるALU18は、入力レジスタ18aと、出力レジスタ18bと、演算部18cとを含んでいる。

【0066】外部から、コントロール回路14の命令レジスタ14bに命令が書き込まれると、コントロール回路14は、その命令に対応して、デジタルLSIチップ10の各回路を制御する。例えばスクランブルキーの解凍であるとする、外部からRAM16に暗号鍵データが書き込まれた後、その鍵の解凍命令が命令レジスタ14bに書き込まれる。

【0067】コントロール回路14は、RAM16の暗号鍵データをALU18の入力レジスタ18aに書き込む。すると、ALU18の演算結果が、出力レジスタ18bに現れる。コントロール回路14は、出力レジスタ18bのデータをゼネラルレジスタ14aに読み込み、スクランブル回路12のレジスタ12cに書き込むという一連のプログラムを実行する。外部からの命令実行が終了すると、コントロール回路14は、その内部のステータスフラグを立て、あるいは割り込みを発生させて外部に通知する。

【0068】デジタルLSIチップ10の製造検査時は、テストモードデータをテスト回路19に与えて、各回路部分毎にテストができるようにする。例えばスクランブル回路12をテストする場合には、ホストI/F回路13を介してスクランブル回路12の全てのレジスタが外部からアクセスできるように、内部接続が制御される。

【0069】その後、仮のスクランブルキーをレジスタ12cに書き込み、仮の規定データを入力データとしてシャッフル回路12aに供給する。そして、所定の期待値データが出力データとして得られるか否かを判別する。もし、スクランブル回路12の一部が不良であった場合には、出力データが期待値と異なるので不良品であると判断することができる。ALU18についても同様な手法でテストすることができる。

【0070】ここで、スクランブル回路12のレジスタ12c、コントロール回路14のゼネラルレジスタ14

a及びALU18の出力レジスタ18bには、秘匿すべきデータがそれぞれラッチされているため、これらレジスタ12c、14a、18bの内容を外部からアクセスできないようにすることが、肝要なことになる。

【0071】上記したセキュリティ回路21によって、ディスエーブル信号がHレベルのとき、内部の回路を自由に外部からアクセス可能とし、ディスエーブル信号がLレベルのとき、上記レジスタ12c、14a、18bの内容を外部からアクセスできないように設定することで、テストを容易に行なうことができ、しかも秘匿データを確実に保護することができるようになる。なお、この発明は上記した実施の形態に限定されるものではなく、この外その要旨を逸脱しない範囲で種々変形して実施することができる。

【0072】

【発明の効果】以上詳述したようにこの発明によれば、秘匿データに対しては外部からのアクセスを確実に阻止することができ、テスト時には信頼性の高い検査を容易に行ない得るようにした極めて良好なデジタル集積回路を提供することができる。

【図面の簡単な説明】

【図1】この発明に係るデジタル集積回路の実施の形態を示すブロック構成図。

【図2】同実施の形態における要部の一例を示すブロック構成図。

【図3】同実施の形態における要部の他の例を示すブロック構成図。

【図4】同実施の形態における要部のさらに他の例を示すブロック構成図。

【図5】同実施の形態におけるメモリのアクセス領域を説明するために示す図。

【図6】同実施の形態におけるスクランブル動作を説明するために示す図。

【図7】同実施の形態におけるデジタルLSIチップを示す外観図。

【符号の説明】

10…デジタルLSIチップ、

11…半導体基板、

12…スクランブル回路、

13…ホストI/F回路、

14…コントロール回路、

15…ROM、

16…RAM、

17…EEPROM、

18…ALU、

19…テスト回路、

20…初期化回路、

21…セキュリティ回路、

22…ワントタイムROM、

23…EXオア回路、

10

20

30

40

50

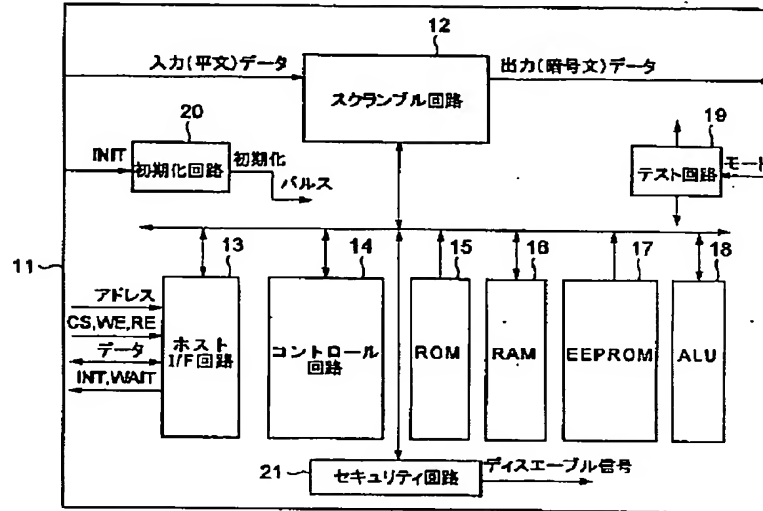
13

14

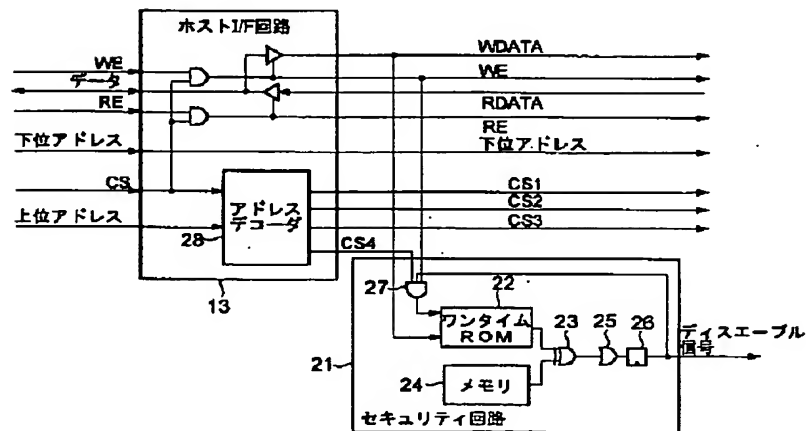
24…メモリ、  
 25…オア回路、  
 26…フリップフロップ回路、  
 27…アンド回路、  
 28…アドレスデコーダ、  
 29…EEPROM、

30…3ステートバッファ、  
 31…アンド回路、  
 32…レジスタ、  
 33…ロジック回路、  
 34…メモリ、  
 35…スイッチ。

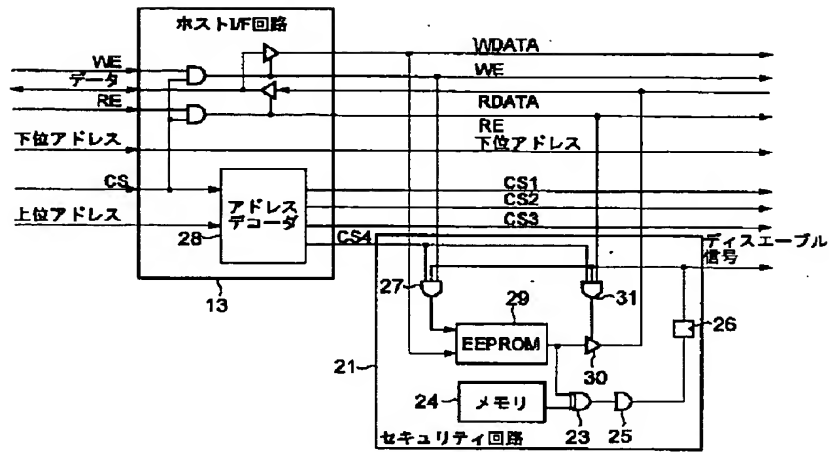
【図1】



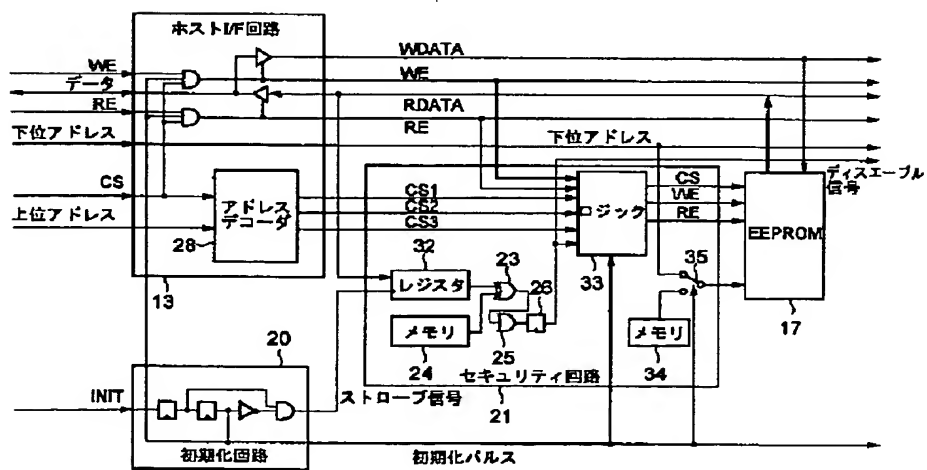
【図2】



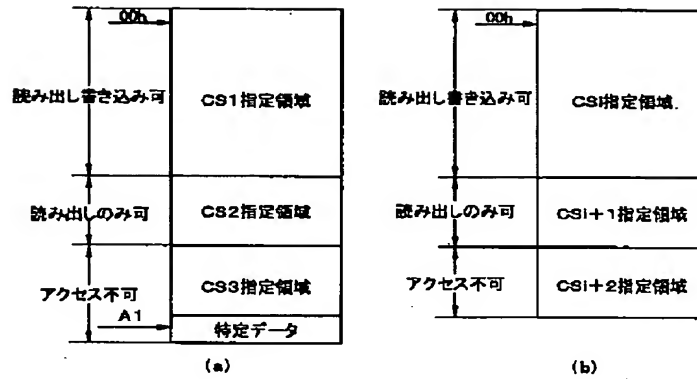
【図3】



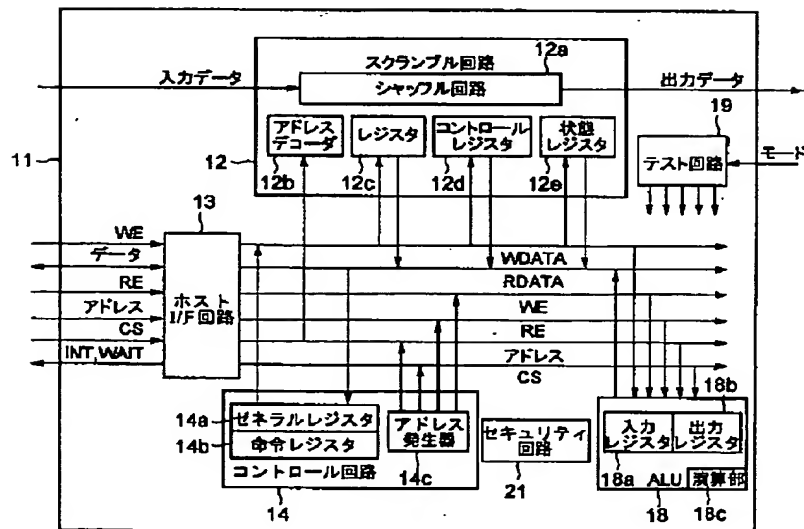
【図4】



【図5】



【図6】



【図7】

